UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,890	09/28/2001	E. David Neufeld	COMP:0224	4334

7590 06/13/2006

Intellectual Property Administration
Legal Dept., M/S35
P.O. Box 272400
Ft. Collins, CO 80527-2400

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 06/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/966,890	NEUFELD ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *March 31, 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-6,9-11,13-19,22-27 and 29-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-6,9-11,13-19,22-27 and 29-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to the Applicant's Amendments and Arguments filed March 31, 2006.

Claims 1, 2, 13, 19, 21, and 28 are amended.

Claims 7, 8, 12 and 20 are cancelled.

Claims 1-6, 9-11, 13-19, 21-32 are herein considered.

Response to Amendment

The Applicant has incorrectly reinstated previously cancelled claims 2, 21, and 28. 37 C.F.R. 1.121(c)(5) states that a previously cancelled claim may be reinstated **only** by adding the claim as a "new" claim with a new claim number. See also 37 C.F.R. 1.126. For purposes of examination, the Examiner has renumbered claims 2, 21, and 28 as 33, 34, and 35 respectively.

Response to Arguments

Applicant's arguments with respect to claims 1, 3-6, 9-11, 13-19, 22-27 and 29-35 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

Claims 1, 3-6, 9-11, and 33 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter because it includes no tangible result.

Claims 13-18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter because it fails to produce any tangible result for those situations in which less than a predetermined portion of the signature value of the seed pool has been altered.

Claims 19, 22-26 and 34 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter because it includes no tangible result.

Claims 27, 29-32, and 35 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter because it fails to produce a tangible result for those situations in which the plurality of data bits has no portion of the signature value.

As per the MPEP, specifically section 2106(2)(a), it is imperative that a claimed invention as a whole accomplishes a practical application and that it produces a "useful, concrete and tangible result." State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02. The purpose of this requirement is to limit patent protection to inventions that possess a certain level of "real world" value, as opposed to subject matter that represents nothing more than an idea or concept, or is simply a starting point for future investigation or research (Brenner v. Manson, 383 U.S. 519, 528-36, 148 USPQ 689, 693-96); In re Ziegler, 992, F.2d 1197, 1200-03, 26 USPQ2d 1600, 1603-06 (Fed. Cir. 1993)). Apart from the utility requirement of 35 U.S.C. 101, usefulness under the patent eligibility standard requires significant functionality to be present to satisfy the useful result aspect of the practical application requirement. See Arrhythmia, 958 F.2d at 1057,

22 USPQ2d at 1036. Merely claiming nonfunctional descriptive material stored in a computer-readable medium does not make the invention eligible for patenting. The claimed invention as a whole must produce a "useful, concrete and tangible" result to have a practical application.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3-6, 9-11, 13-19, 22-27, 29-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bruce Schneier's "Applied Cryptography", hereinafter referred to as *Schneier*, and further in view of US Patent No. 5,680,131 to Utz et al., hereinafter referred to as *Utz*.

Regarding **claim 1**, Schneier discloses a method of generating a random number for a cryptographic security subsystem of a processor-based device, the method comprising the acts of (a) detecting occurrences of a first type of triggering event (SCHNEIER page 426 lines 6-14); (b) writing one or more bits of data to a seed pool (or reservoir) upon termination of the first type of triggering event (SCHNEIER pages 424, 426); (c) detecting occurrence of a second type of triggering event; (d) writing one or

more bits of data to the seed pool upon termination of the second type of triggering event, wherein act (d) comprises masking one or more bits of data to the seed pool upon termination of the second type of triggering event (SCHNEIER page 426 lines 16-17); (e) examining the state bit to determine whether the seed pool is full (page 428 lines 16-18); and (f) if the seed pool is not full, repeating acts (a) through (e) until (enough events have taken place) the seed pool is full (SCHNEIER page 428 lines 16-18).

Schneier fails to *specifically* mention determining if a seed pool is full or masking bits into the seed pool.

Utz discloses the act of masking (serially combining) the one or more bits of data into the seed pool (UTZ col.6 lines 57-61; col.5 line 22) as well as determining if the seed pool is full; and writing one or more bits of data to the seed pool upon termination of the second type of triggering event if the seed pool is not full (UTZ col.3 lines 38-40; col.11 lines 51-55).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Schneier the Utz's ability to determine if a seed pool is full and masking bits into the seed pool in order to allow the cryptographic security subsystem in knowing when the pool is full and available for use in creating a random number.

Regarding **claim 3**, Schneier further discloses that the first type of triggering event has a variable duration (seemingly random events) (SCHNEIER page 426 lines 7-8).

Regarding **claims 4-6**, Schneier further discloses that the processor-based device is coupled to a communication link, and includes the act of receiving a communication from the communication link (arrival times of network packets), the link comprising a plurality of types (network, multimedia, etc) (SCHNEIER page 426 lines 14-27).

Regarding **claim 9,** Schneier further discloses that act (d) comprises capturing the one or more bits of data from a free-running timer upon termination of the second type of triggering event (SCHNEIER 426 lines 37-34).

Regarding **claim 10**, Schneier further discloses that the second type of triggering event is different than the first type of triggering event (as many good sources of randomness as are available) (SCHNEIER 426 lines 37-34).

Regarding **claim 11**, Schneier further discloses that the second type of triggering event is a cycle of power applied to the processor-based device (SCHNEIER page 426 lines 12-13).

Regarding **claim 13**, Utz discloses a method of initializing a seed pool for generating a random number for a cryptographic security subsystem of a processor-based device, the method comprising the acts of (a) prior to enabling the cryptographic security subsystem, writing a plurality of bits of data to a seed pool (RS/PRNG), the plurality of bits of data having a signature (start) value (UTZ col.5 lines 34-42; col.6 lines 13-28); (b) detecting occurrences of a first type of triggering event and (c) writing one or more bits of data to the seed pool upon termination of the first type of triggering event, the one or more bits of data altering the signature value of the seed pool (col.6 lines 37-

61); and (d) enabling the cryptographic security subsystem when more than a predetermined portion of the signature value of the seed pool has been altered (UTZ col.7 line 61thru col.8 line 13; col.9 line 62 thru col.10 line 16).

Regarding **claims 14 and 15**, Utz discloses wherein the first type of triggering event comprises either a cycle of power applied to the processor-based device or a reboot of the processor-based device (power-on reset circuit) (UTZ col.5 lines 57-67).

Regarding **claim 16**, Utz discloses wherein act (c) comprises the act of masking (serially combining) the one or more bits of data into the seed pool (UTZ col.6 lines 57-61; col.5 line 22).

Regarding **claim 17**, Utz discloses wherein act (c) comprises the act of capturing the one or more bits of data from a free-running timer (clock signals) (UTZ col.5 lines 59-61) .

Regarding **claim 18**, Utz discloses detecting a second type of triggering event; determining if the seed pool is full; and writing one or more bits of data to the seed pool upon termination of the second type of triggering event if the seed pool is not full (UTZ col.3 lines 38-40; col.11 lines 51-55).

Claim 19 is directed towards a device's implementation of the method of claim 1 and is rejected by similar rationale.

Claim 22 is directed towards a device's implementation of the method of claim 3 and is rejected by similar rationale.

Claim 23 is directed towards a device's implementation of the method of claim 4 and is rejected by similar rationale.

Claim 24 is directed towards a device's implementation of the method of claim 5 and is rejected by similar rationale.

Regarding **claim 25**, Utz discloses wherein the interface controller comprises an RS232 interface controller (UTZ col.7 lines 41-45; col.10 lines 48-53).

Claim 26 is directed towards a device's implementation of the method of claim 11 and is rejected by similar rationale.

Regarding **claim 27**, Utz discloses a processor-based device comprising: a host processing system, the host processing system comprising a processor and a communications management system in communication with the host processing system (UTZ col.5 lines 52-67); and a memory system in communication with the host processing system and the communications management system, wherein the communications management system comprises: an interface controller (UTZ col.6 lines 8-12); a non-volatile memory device to store a seed pool comprising a plurality of data bits (UTZ col.5 lines 34-42); and security logic in communication with the interface controller and the non-volatile memory device, the security logic configured to establish a secure communication session between the processor-based device and an external device in communication with the processor-based device via the interface controller (UTZ col.4 lines 47-60), and wherein the security logic is configured to: write the one or more bits to the seed pool , the bits altering a signature value; determine whether the plurality of data bits in the seed pool has at least a portion of a signature value; and disable establishment of the secure communication session if the plurality of data bits has at least a portion of the signature value (UTZ col.9 line 62 thru col.10 line 16).

Regarding **claim 29**, Utz discloses a main power supply to supply power to the processor-based device, and wherein the first type of triggering event comprises a cycle of the power supplied by the main power supply (power-on reset circuit) (UTZ col.5 lines 57-67).

Regarding **claims 30-31**, Utz discloses wherein the security logic is configured to detect a second type of triggering event; determine whether the seed pool is fully populated; and write one or more data bits to the seed pool upon termination of the second type of triggering event if the seed pool is not fully populated (UTZ col.3 lines 38-40; col.11 lines 51-55) and wherein the second type of triggering event comprises receipt of a communication from the external device via the interface controller (UTZ col.3 lines 38-40; col.11 lines 51-55).

Regarding **claim 32**, Utz discloses wherein the interface controller comprises a network interface controller (UTZ col.7 lines 41-45; col.10 lines 48-53).

Regarding **claim 33** (cancelled claim 2), Schneier further discloses the act of capturing one or more bits of data from a free-running timer (most finely grained time-of-day clock, for example the Intel 8254 clock chip) upon termination of the first type of triggering event (SCHNEIER page 426 lines 27-34).

Claim 34 (cancelled claim 21) is directed towards a device's implementation of the method of claim 33 (cancelled claim 2) and is rejected by similar rationale.

Regarding **claim 35** (cancelled claim 28), Utz discloses wherein the security logic is configured to detect a first type of triggering event, and to write one or more data bits

to the seed pool upon termination of the first type of triggering event (UTZ col.6 lines 37-61).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TT/EMM
June 9, 2006

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER